CLAIMS:

1	1.	A method for reducing the boot time of a Trusted Computing Performance		
2	Allia	Alliance (TCPA) based computing system comprising the steps of:		
3		resetting said TCPA computing system;		
4		executing a boot block code comprising a Core Root of Trust Measurement		
5	(CRT	(CRTM);		
6		reading bits in a register of a flash memory storing said boot block code,		
7	where	ein said bits in said register indicate whether segments of said flash memory		
8	have	have been updated; and		
9		obtaining one or more measurement values from a table storing hashed values		
10	from a previous measurement of a Power On Self Test (POST) Basic Input/Output			
11	Syste	System (BIOS) if one or more of said bits read in said register indicate one or more of		
12	said s	egments of said flash memory storing said POST BIOS have not been updated.		
1	2.	The method as recited in claim 1 further comprising the step of:		
2		transmitting said obtained measurement values to a Trusted Platform Module.		
1	3.	The method as recited in claim 2 further comprising the steps of:		
2		setting a control bit in said register so no other device can set said bits read in		
3	said r	egister; and		
4		executing said POST BIOS.		
1	4.	The method as recited in claim 1 further comprising the steps of:		
2		performing a measurement of a segment of said flash memory storing said		
3	POST	BIOS which is indicated by a bit in said register as having been updated;		
4		performing a look-up in said table of a previous measurement of said segment		
5	updat	ed of said flash memory storing said POST BIOS; and		
6	-	comparing said measured value with said looked-up value in said table.		
		·		

1	5.	The method as recited in claim 4 further comprising the step of:
2		taking appropriate security measures if said measured value is not equal with
3	said l	ooked-up value in said table.

- 6. The method as recited in claim 4 further comprising the step of:
 resetting said bit in said register to indicate that said segment of said flash
 memory is validated if said measured value is equal with said looked-up value in said
 table.
- 7. The method as recited in 6 further comprising the step of:

 transmitting said measured value of said segment of said flash memory
 updated and said obtained measurement values of one of more of said segments of
 said flash memory storing said POST BIOS that have not been updated to a Trusted
 Platform Module.

1	8. A computer program product embodied in a machine readable medium for	
2	reducing the boot time of a Trusted Computing Performance Alliance (TCPA) base	
3	computing system comprising the programming steps of:	
4	executing a boot block code comprising a Core Root of Trust Measurement	
5	(CRTM);	
6	reading bits in a register of a flash memory storing said boot block code,	
7	wherein said bits in said register indicate whether segments of said flash memor	
8	have been updated; and	
9	obtaining one or more measurement values from a table storing hashed values	
10	from a previous measurement of a Power On Self Test (POST) Basic Input/Output	
11	System (BIOS) if one or more of said bits read in said register indicate one or more of	
12	said segments of said flash memory storing said POST BIOS have not been updated.	
1 .	9. The computer program product as recited in claim 8 further comprising the	
2	programming step of:	
3	transmitting said obtained measurement values to a Trusted Platform Module.	
1:	10. The computer program product as recited in claim 9 further comprising the	
2	programming steps of:	
3	setting a control bit in said register so no other device can set said bits read in	
4	said register; and	
5	executing said POST BIOS.	
1	11. The computer program product as recited in claim 8 further comprising the	
2	programming steps of:	
3	performing a measurement of a segment of said flash memory storing said	
4	POST BIOS which is indicated by a bit in said register as having been updated;	
5	performing a look-up in said table of a previous measurement of said segment	
6	updated of said flash memory storing said POST BIOS; and	
7	comparing said measured value with said looked-up value in said table.	

1	12.	The computer program product as recited in claim 11 further comprising the	
2	progra	programming step of:	
3		taking appropriate security measures if said measured value is not equal with	
4	said looked-up value in said table.		
	1		
1	13.	The computer program product as recited in claim 11 further comprising the	
2	programming step of:		
3		resetting said bit in said register to indicate that said segment of said flash	
4	memo	memory is validated if said measured value is equal with said looked-up value in said	
5	table.		
1	14.	The computer program product as recited in 13 further comprising the	
2	progra	programming step of:	
3		transmitting said measured value of said segment of said flash memory	
4	update	updated and said obtained measurement values of one of more of said segments of	
5	said fl	ash memory storing said POST BIOS that have not been updated to a Trusted	

6

Platform Module.

1	15. A system, comprising:	
2	a processor;	
3	a Trusted Building Block (TBB) coupled to said processor, wherein said TBB	
4	is configured to ensure integrity of said system, wherein said TBB comprises:	
5	a Trusted Platform Module (TPM) configured to implement	
6	cryptographic algorithms; and	
7	a portion of a flash memory coupled to said TPM, wherein said flash	
8	memory in said TBB comprises:	
9	a register comprising bits configured to indicate whether	
10	segments of said flash memory have been updated;	
11	a table configured to store measurements of a Power On Self	
12	Test (POST) Basic Input/Output System (BIOS) code stored in one or more segments	
13	of said flash memory; and	
14	a boot block code, wherein said boot block code comprises	
15	code to reset said system, wherein said boot block code comprises a Core Root of	
16	Trust for Measurement (CRTM) configured to measure said POST BIOS code;	
17	wherein said processor, responsive to said CRTM, comprises:	
18	circuitry operable for executing said boot block code;	
19	circuitry operable for reading said bits in said register of said flash	
20	memory; and	
21	circuitry operable for obtaining one or more measurement values from	
22	said table if one or more of said bits read in said register indicate one or more of said	
23	segments of said flash memory storing said POST BIOS code have not been updated.	
1	16. The system as recited in claim 15, wherein said processor further comprises:	
2	circuitry operable for transmitting said obtained measurement values to said	
3	TPM.	

1	17.	The system as recited in claim 16, wherein said processor further comprises:	
2		circuitry operable for setting a control bit in said register so no other device	
3	can set said bits read in said register; and		
4		circuitry operable for executing said POST BIOS code.	
1	18.	The system as recited in claim 15, wherein said processor further comprises:	
2		circuitry operable for performing a measurement of a segment of said flash	
3	memo	ory storing said POST BIOS code which is indicated by a bit in said register as	
4	having	having been updated;	
5		circuitry operable for performing a look-up in said table of a previous	
6	measurement of said segment of said flash memory storing said POST BIOS code;		
7	and		
8		circuitry operable for comparing said measured value with said looked-up	
9	value in said table.		
1	19.	The system as recited in claim 18, wherein said processor further comprises:	
2		circuitry operable for taking appropriate security measures if said measured	
3	value	is not equal with said looked-up value in said table.	
1	20.	The system as recited in claim 18, wherein said processor further comprises:	
2		circuitry operable for resetting said bit in said register to indicate that said	
3	segment of said flash memory is validated if said measured value is equal with said		
4	looked-up value in said table.		
1	21.	The system as recited in claim 20, wherein said processor further comprises:	
2		circuitry operable for transmitting said measured value of said segment of said	
3 .	flash	memory updated and said obtained measurement values of one or more of said	
	segments of said flash memory storing said POST BIOS code that have not been		
4	Segine	and of bala main memory blotting bala 1 001 2100 bela mar have not been	